

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau(43) International Publication Date
22 April 2004 (22.04.2004)

PCT

(10) International Publication Number
WO 2004/034633 A2(51) International Patent Classification⁷: H04L 9/28(21) International Application Number:
PCT/GB2003/004401

(22) International Filing Date: 10 October 2003 (10.10.2003)

(25) Filing Language: English

(26) Publication Language: English

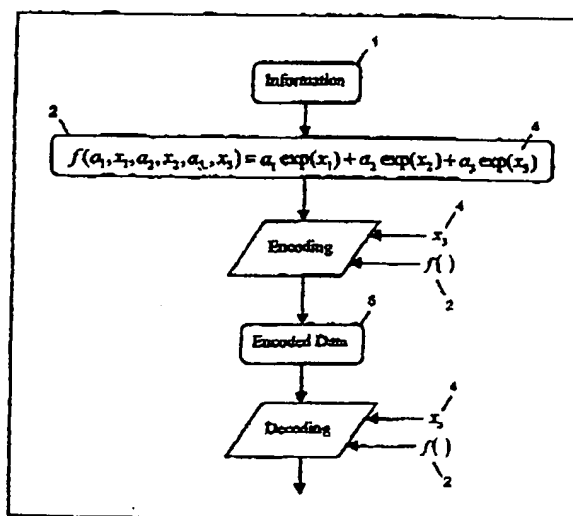
(30) Priority Data:
0223692.5 11 October 2002 (11.10.2002) GB(71) Applicant (for all designated States except US): MULTI-
PLEX PHOTONICS LIMITED [GB/GB]; Unit 8 Green-
heys Centre, Manchester Science Park, Manchester M15
6JJ (GB).

(72) Inventors; and

(75) Inventors/Applicants (for US only): REGA, Carlos,
Alberto [ES/GB]; 13 Wood Street, Hollingworth, Hyde,
Cheshire SK14 8NL (GB). LLOYD, Christopher,
James [GB/GB]; 117 Market Street, Hollingworth, Hyde,Cheshire SK14 8TY (GB). KLARKE, David, John
[GB/GB]; 6 Fields Drive, Sandbach, Cheshire CW11 1YB
(GB). VARNHAM, Malcolm, Paul [GB/GB]; 76 Grange
Road, Alresford, Hampshire SO24 9HF (GB).(74) Agent: JONES, Graham, Henry; Graham Jones & Com-
pany, 77 Beaconsfield Road, Blackheath, London SE3 7LG
(GB).(81) Designated States (national): AE, AG, AL, AM, AT, AU,
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,
CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE,
GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR,
KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK,
MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT,
RO, RU, SC, SD, SE, SG, SK, SL, SY, TI, TM, TN, TR,
TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.(84) Designated States (regional): ARIPO patent (GH, GM,
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),
Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,
ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO,
SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM,
GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: APPARATUS AND METHOD OF ENCODING AND DECODING INFORMATION



(57) Abstract: A method for encoding and decoding information, the method comprising the steps of: (a) using at least one mathematical function; (b) producing an encryption algorithm using the mathematical functions such that the algorithm has at least two parameters; (c) defining a decode key of a data stream by defining the value of at least one parameter; (d) defining information to be carried in a data stream by defining the value of at least one parameter; (e) producing a data stream using the encryption algorithm and the defined parameter values; and (f) decrypting the data stream where the decode key is known and used as a constraint in the equation such that the information is available, wherein the encryption algorithm is selected such that decoding of the encryption algorithm would be ill-conditioned without the constraint.

BEST AVAILABLE COPY

WO 2004/034633 A2